This document provides the specifications of the Service Level Agreements (SLA) monitoring and managing functionalities for the SecureIoT Security as a Service (SECaaS) services. It also illustrates how it can be implemented and integrated in the SecureIoT platform in-line with the SecureIoT architecture and security data models.
Executive Summary

SecureIoT is developing a data-driven platform for securing Internet of Things (IoT) systems and services. The platform adheres to the main structuring principles of popular reference architectures for IoT systems and services such as the Industrial Internet Security Framework (IISF) and implements monitoring, analysis and actuation security workflows based on the collection and processing of security-related data from IoT systems and devices. SecureIoT offers three main types of security services for IoT assets, including risk assessment services, compliance auditing services and developers’ support services. The latter services are designed and implemented as cloud-based security services i.e. as services that are implemented based on the Security-as-a-Service (SECaaS) paradigm. The SECaaS model involves at least an owner or operator of an IoT system (e.g., a platform and/or service and/or device) and the provider of the security service in the cloud. As such it also implies the establishment and management of a proper Service Level Agreement (SLA) between the parties that are entailed in the SECaaS service. In this context, the present deliverable provides an initial specification of SecureIoT SLAs, including their parameters and how they can be managed in the scope of the SecureIoT platform operation.

The deliverable starts with an introduction to the merit and need for establishing SLAs between the providers and the users of the SecureIoT SECaaS services. In this direction, it illustrates a set of business scenarios that serve as a reference for specifying and implementing the SecureIoT SLA Management mechanisms. The most sophisticated of these scenarios involve the protection of IoT services that span multiple IoT platforms, which means that they are provided by more than one operators of IoT systems. Such scenarios are typical in IoT services that span a value chain.

A central part of the deliverable is devoted to the specification of the main parameters of an SLA that have to be managed by the SecureIoT platform. These parameters serve as a basis for establishing an SLA. However, they are also used for monitoring, tracking and auditing the SLA during the provision of SECaaS services. As part of the auditing process, the SecureIoT platform should ensure that the business entities which engage in the SLA provide/access data and services in-line with their rights and obligations, as the latter are specified in the SLA.

The document presents also how the SLA management mechanisms can be implemented and integrated in the SecureIoT platform. To this end, an SLA management module (consisting of an SLA Processing Engine and of repository of SLA information) has been defined, along with the way it can be integrated with other components of the SecureIoT architecture. The SLA management module maintains information on the establishment, activation and deactivation of SLAs. At the same time, it tracks the data exchanged between the IoT system provider and the SECaaS services provider. The latter data include security information flows provided for the IoT system(s) that are to be protected, as well as risk assessment, compliance auditing and other reports that are generated by the SECaaS services.
Key to the implementation of the SLA management module is the modelling of an SLA object that represents an SLA within the SecureIoT platform. This model is integrated to the SecureIoT data model that has been specified in other deliverables of WP3 and WP4 of the project.

Note that this deliverable represents the first version of the specification of the SLA management modules and mechanisms of the project. A second version is planned during the third year of the project’s lifetime and shall provide updates and improvements to these mechanisms based on feedback from the initial deployment and use of the SECaaS services. The next version of the deliverable will also consider the exploitation models and business planning activities of the project, as these are likely to specify the business interactions between the SECaaS services providers and their customers i.e. interactions directly related to the SLA mechanisms. While both deliverables are marked as reports in the Description of the Action (DoA), the SecureIoT consortium will endeavour to provide a proof of concept implementation of the SLA management mechanisms as part of its platform.
### Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Contributor(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>13/05/2019</td>
<td>Sofoklis Efremidis, John Soldatos</td>
<td>Document Structure, Table of Contents</td>
</tr>
<tr>
<td>0.2</td>
<td>03/06/2019</td>
<td>Sofoklis Efremidis, John Soldatos</td>
<td>First content</td>
</tr>
<tr>
<td>0.3</td>
<td>23/06/2019</td>
<td>Sofoklis Efremidis, John Soldatos</td>
<td>Revised content, scenario completion, SLAs</td>
</tr>
<tr>
<td>0.35</td>
<td>24/06/2019</td>
<td>Sofoklis Efremidis, John Soldatos</td>
<td>Update of Section 2 based on indicative Business Scenarios</td>
</tr>
<tr>
<td>0.4</td>
<td>25/06/2019</td>
<td>Sofoklis Efremidis, John Soldatos</td>
<td>Update of Section 3 regarding SLA Management functionalities and alignment to SecureIoT architecture</td>
</tr>
<tr>
<td>0.5</td>
<td>26/06/2019</td>
<td>Sofoklis Efremidis, John Soldatos</td>
<td>Update of Section 4 regarding SLA Objects specifications and implementation</td>
</tr>
<tr>
<td>0.6</td>
<td>27/06/2019</td>
<td>Sofoklis Efremidis, John Soldatos, A. Despotopoulou</td>
<td>Updates of Section 4, regarding enhancements to SecureIoT architecture for SLA management</td>
</tr>
<tr>
<td>0.7</td>
<td>03/07/2019</td>
<td>Sofoklis Efremidis, John Soldatos, A. Despotopoulou</td>
<td>Updates to Sections 3 &amp; 4, regarding SLA parameters and their modelling</td>
</tr>
<tr>
<td>0.8</td>
<td>04/07/2019</td>
<td>Sofoklis Efremidis, John Soldatos, A. Despotopoulou</td>
<td>Preparation of Version for Quality Control</td>
</tr>
<tr>
<td>0.9</td>
<td>04/07/2019</td>
<td>Sofoklis Efremidis, John Soldatos, A. Despotopoulou</td>
<td>Additional Information on the SLA Data Modelling</td>
</tr>
<tr>
<td>0.95</td>
<td>09/07/2019</td>
<td>Jurgen Nieses, Hendrik Eikerling</td>
<td>Quality Reviewed Version</td>
</tr>
<tr>
<td>0.99</td>
<td>10/07/2019</td>
<td>John Soldatos</td>
<td>Updates &amp; Revision following Quality Review – Version for Delivery to EC</td>
</tr>
<tr>
<td>1.0</td>
<td>12/07/2019</td>
<td>John Soldatos</td>
<td>Fine Tuning of Appendix and Updates on the Business Incentives Section</td>
</tr>
</tbody>
</table>
Table of Contents

Executive Summary .......................................................................................................................... 2

Definitions, Acronyms and Abbreviations ...................................................................................... 9

1 Introduction ..................................................................................................................................... 10
   1.1 Background and Vision ............................................................................................................. 11
   1.2 Security Services ....................................................................................................................... 12
   1.3 SecureIoT Architecture ............................................................................................................ 13
   1.4 Methodology ............................................................................................................................ 14
   1.5 Relationship to other Deliverables ............................................................................................ 15
   1.6 Document Structure .................................................................................................................. 16

2 Motivation for SLA Management ................................................................................................... 17
   2.1 The SecureIoT SECaaS Services ............................................................................................... 17
   2.2 Business Actors entailed in SecureIoT Services ......................................................................... 18
   2.3 Indicative Business Scenarios involved SLAs and their Management ....................................... 20
      2.3.1 Scenario #1: SECaaS Services for IoT Device Protection .................................................. 20
      2.3.2 Scenario #2: SECaaS Services for IoT Platform Protection .............................................. 21
      2.3.3 Scenario #3: SECaaS Services for IoT Development ........................................................ 22
      2.3.4 Scenario #3: SECaaS Services for IoT Service Protection ............................................... 22
      2.3.5 Scenario #4: SECaaS Multi-Platform Protection ............................................................... 22

3 Functional Specifications of SLA Management in SecureIoT ....................................................... 25
   3.1 Overview ................................................................................................................................... 25
   3.2 SLA Management Module Specification .................................................................................... 25
      3.2.1 Identification – SLA ID ......................................................................................................... 25
      3.2.2 Participating Entities ............................................................................................................ 25
      3.2.3 SLA Type ............................................................................................................................. 26
      3.2.4 SECaaS Services Type ........................................................................................................ 26
      3.2.5 Tracking of Data Collection Information .............................................................................. 26
      3.2.6 Tracking of SECaaS Outputs ............................................................................................. 27
      3.2.7 Notifications & Alerts ......................................................................................................... 27
      3.2.8 Reconfiguration .................................................................................................................... 27
      3.2.9 Accounting and Utility Metrics ............................................................................................ 28
3.2.10 Security Requirements
3.2.11 Other SLA Information
3.2.12 Business Incentives Tracking & Implementation

4 SLA Management Design and Implementation
   4.1 SLA Management Module Data Models
   4.2 Integration in the SecureIoT Architecture

5 Conclusions

References

Appendix A. SLA Data Models Structure
List of Figures

FIGURE 1: OVERALL SecureIoT ARCHITECTURE (WITHOUT SLA ENHANCEMENTS) ................................................................. 13
FIGURE 2: METHODOLOGY AND MAIN ACTIVITIES ENTAILED IN THE SPECIFICATION AND IMPLEMENTATION OF SLA MANAGEMENT IN SecureIoT ........................................................................ 15
FIGURE 3: BUSINESS SCENARIO: OEM & SECAAS PROVIDER SLA .................................................................................. 21
FIGURE 4: BUSINESS SCENARIO: IOT PLATFORM PROVIDER & SECAAS PROVIDER SLA .................................................. 21
FIGURE 5: SUPPLY CHAIN MULTI IOT PLATFORM SCENARIO ......................................................................................... 23
FIGURE 6: SecureIoT ARCHITECTURE ENHANCED WITH THE BUILDING BLOCKS FOR SLA MANAGEMENT ....................... 31
FIGURE 7: STRUCTURE OF SecureIoT DATA MODEL (SECIoT-DM) AND PLACEMENT OF SLA GROUP IN IT ..................... 35
FIGURE 8: STRUCTURE SLA GROUP – SLA ROOT ELEMENT ......................................................................................... 36
FIGURE 9: SLA OBJECT DEFINITION .......................................................................................................................... 37
FIGURE 10: SLA OBJECT ............................................................................................................................................. 38
FIGURE 11: COMPLEX SLA OBJECT ........................................................................................................................... 39
FIGURE 12: STRUCTURE OF SLA REPORT .................................................................................................................... 40
List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>Input and Outputs of the SECaaS Services</td>
<td>18</td>
</tr>
<tr>
<td>Table 2</td>
<td>Overview of Business Roles Entailed in the Provision of an IoT SECaaS Service and Associated SLA Management Functionalities</td>
<td>19</td>
</tr>
</tbody>
</table>
## Definitions, Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAS</td>
<td>Compliance Auditing Service</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
</tr>
<tr>
<td>CRUD</td>
<td>Create Read Update Delete</td>
</tr>
<tr>
<td>DoA</td>
<td>Description of Action</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Directive</td>
</tr>
<tr>
<td>IISF</td>
<td>Industrial Internet Security Framework</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IoTSP</td>
<td>IoT Service Provider</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technologies</td>
</tr>
<tr>
<td>NVD</td>
<td>National Vulnerability Database</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SECaaS</td>
<td>Security as a Service</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SME</td>
<td>Small Medium Enterprise</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>XACML</td>
<td>eXtensible Access Control Markup Language</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language</td>
</tr>
</tbody>
</table>
1 Introduction

The main goal of SecureIoT is to introduce, validate and promote a novel approach to securing IoT applications. This approach emphasizes a timely, predictive and intelligent approach to the identification and mitigation of security threats and incidents. One of main characteristics of this approach is its ability to deal with smart objects, while at same time supporting security interoperability in supply chain scenarios that involve multiple IoT systems and platforms with diverse security capabilities. The project reflects its approach into an architectural concept, which serves as a basis for implementing predictive and intelligent security systems. Based on this overarching architectural concept, the project develops concrete security services that will be validated in the scope of the project’s use cases.

The SECaaS security services are supported by a platform that uses predictive security analytics for Internet-of-Things (IoT) deployments and applications to detect security threats and raise alerts, enforce policies and the appropriate reconfigurations to the target IoT deployment. This approach employs the classical Monitor→Analyze→Act security workflow, which cycles through the collection of security data, their analysis, and respective responses when threats are detected.

The provision of SECaaS services in the context of SecureIoT requires that:

- **An IoT system owner provides security related data about the system that it owns.** In this context, the term IoT system may range from a single IoT device or platform, to an entire set of interconnected systems that support a value chain.

- **The business entity (i.e. SecureIoT services provider) that offers the SECaaS services processes these data and provides security services to the IoT system owner.** Depending on the type of the SECaaS service provided, the SECaaS service will provide and/or visualize some outputs to the IoT system owner, like a compliance report, a risk assessment for some IoT assets or a security alert.

In this context any interaction between an IoT system owner/operator and the SecureIoT SECaaS services providers implies a set of business interactions between these two entities. These business interactions have some implications in the technical interactions between the systems of the entities i.e. the IoT devices and platforms of the IoT system owner (i.e. the SECaaS customer) and security platform of the SECaaS service provider. These business and technical interactions are governed by appropriate Service Level Agreements (SLAs) between the business entities and their technical systems.

This is the case with all cloud-based services, including cloud services that entail IoT data and devices (e.g., [Soldatos14], [Gaillard14]). In general, SLAs are integral elements of all models of cloud-based services delivery. They reflect a common understanding between the parties that engage in the provision of any cloud service in the following areas:

- The service or services offered by the provider(s) to the customer(s).
- The priorities of the different services.
- The rights and responsibilities of the participating business entities.
- Any guarantees associated with the delivery of the service.
• Warranties and licensing agreements.

Hence, an SLA deals with the services to be delivered, their performance, the way the SLA is tracked and reported, how problems are managed, how confidential information is handled, what’s the lifecycle of the agreement (e.g., when and under which conditions it can be terminated), as well as legal matters such as compliance and resolution of disputes. For example, in the cloud computing paradigm, SLAs define a grade of service in terms of availability, serviceability, performance and other attributes, while being associated with some billing plan.

This deliverable is destined to drill down on the details of these SLAs, as a means of specifying how they should be implemented in order to enabling the practical deployment of SECaaS services through the SecureIoT platform. In particular, the deliverable focuses on:

• Analyzing the implications of the main SecureIoT deployment scenarios on the SLAs between IoT systems owners, IoT systems operators and SecureIoT service providers.
• Specifying how the SecureIoT SLA management mechanisms could be implemented in-line with the SecureIoT architecture.

The scope of SLA management in SecureIoT (and therefore in this document as well), goes beyond conventional cloud computing and focuses on the grade of the security services that are delivered based on the SECaaS modality. Parameters associated with conventional cloud computing SLAs (e.g., the availability and performance of the cloud-based SECaaS services) are still applicable, but out of the scope of this deliverable. They fall in the realm of cloud computing services and are expected to be handled in a way similar to most cloud services.

A key advantage of the SecureIoT services is that they can be used in a multi IoT platform deployment. Along with an overview of the SecureIoT SLA management and mechanisms this document explores the implications as well as the advantages of providing services in such an environment. It discusses the motivations for the entities that own IoT platforms over which an IoT application is deployed to provide security data as well as the terms and conditions under which such data are provided. Typically, interactions between multiple entities are also governed by Service Level Agreements (SLAs), which are enforced by appropriate monitoring mechanisms. This is also the case for the provision of security data to the SecureIoT platform as will be discussed in following paragraphs.

The deliverable illustrates also the value of data collection and provision for the delivery of data-intensive SECaaS services. In this context, the SLA management functionalities of SecureIoT will allow for the implementation of incentive-based schemes for SECaaS customers to provide as many data as possible i.e. data beyond the minimum required for the delivery of a SECaaS service.

1.1 Background and Vision

The vision of the SecureIoT project is to provide new insights on security monitoring and data-driven security intelligence for multi-platform IoT systems, through enabling the implementation of predictive security systems that can analyse data from IoT platforms and smart objects (i.e. objects with semi-autonomous behaviour). Hence, the components for exchanging data between
the SecureIoT platform and the deployment IoT platforms should be introduced into the overall architecture and the corresponding mechanisms implemented.

1.2 Security Services

The SecureIoT services for IoT based applications include Risk Assessment, Compliance Auditing, and Developer Support. In the course of the project, three representative use cases will validate the SecureIoT services: (a) multivendor Industry 4.0 application, (b) connected cars and autonomous vehicles, and (c) social assistive robots. For the three use cases as well as any applications that may make use of the SecureIoT services, there are two visible points of interaction with the SecureIoT platform.

The first is the set of security services that are provided by it, as follows:

- **Risk Assessment**: a set of services for the quantification of risks to which an IoT deployment or application may be exposed to, based on the probability and impact each one may have. The NIST CVSS (Common vulnerability Scoring System) will be used for this service.

- **Compliance Auditing**: a set of services that support auditing of IoT deployments and services against existing sets of security and privacy controls. Auditing services depend on data collected from the IoT deployment. Auditing requirements may include policies that need to be complied with and may also be expressed in XACML. The auditing service outputs sets of issues in which compliance may be at risk and require further attention.

- **Developer Support**: a set of services for secure IoT programming based on programming annotations that extend and complement existing programming constructs. The services will be expressive enough to allow for enforcement of policies at various levels of the IoT target deployment, i.e., device, smart object, edge, cloud. The developer support services are mapped into controls of the target IoT deployment or application and are used during its operation.

The second point of interaction of an IoT deployment or application with the SecureIoT platform is through the mechanisms used for those services. Monitoring of the target IoT deployment is the basis for the provided security services and as a consequence the collection of security data from its various levels and their transfer to the SecureIoT platform for processing is mandatory. In particular, security data collection and processing is necessary for supporting the risk assessment and compliance auditing services.

The SecureIoT services are supported by a number of internal services and components. The main ones include:

- **Security Analytics**: the service operates on collected security data and tries to find patterns in them that may be deemed suspicious resulting to the raise of alerts. Security
contextual data in the form of templates may also be used for tuning the analytics process to the context to which it is applied.

- Security Knowledge Base: it contains security related data, in particular those related to cyber threats. The corresponding CTI graphs are used by the security analytics that must maintain an up-to-date knowledge of cyber thread.
- Policy Management: it is a repository for the policy models and provides functionalities for their management and or for policy interoperability. Moreover, it supports the definition of trustworthiness metrics and provides programming support for expressing security requirements.
- SecureIoT Data Store: it is a repository of the deployed probes as well as the assets of the target IoT deployment. Moreover, it contains cyber-threat and vulnerability data and the policies to be enforced.

1.3 SecureIoT Architecture

The SecureIoT architecture is presented in Deliverable D2.5. In that document the 4+1 architectural view is used to provide complementary views of the architecture. A logical view of the overall SecureIoT architecture is summarized in Figure 1.

![Figure 1: Overall SecureIoT architecture (without SLA Enhancements)](image)

As shown, the operation of the architecture is facilitated by a data bus for the communication between its components. The main parts of the architecture are described below.

- Data collection and streaming. The component is responsible for collecting data from the parts of the target IoT deployment. Its main subcomponents are:
  - Deployed probes: they collect data from the target IoT deployment or application and stream them to the IoT platform through the data routing component.
  - Probe management and configuration: the component is responsible for managing and configuring the deployed probes. It interacts with SPEP from which
it receives automatic probe configuration commands and correspondingly configures the managed probes. Manual probe configuration commands may also be received by the dashboard.

- Probe registry: it is a registry of the deployed probes. Probe deployment data, as well as state and configuration data are maintained by the registry. The registry provides probe creation, reconfiguration and search capabilities.

- Databases: they provide persistent storage to the rest of the platform components. They comprise the following
  - Global database: it contains the data collected by the deployed probes.
  - Asset configuration data: it is a registry of the assets of the target IoT deployment and along with configuration data.
  - Policy repository: contains the policies that are to be enforced to the target IoT deployment

- Analytics engine: Provides security analytics functionalities based on the collected security data as well as training data and templates. It makes use of the templates database that contains contextual security data.

- Compliance Auditing Service: it checks and verifies the compliance of the target IoT deployment to regulatory related requirements, e.g., GDPR, NIS, etc. The service operates on collected security data as well as regulatory requirements that are expressed as policies. The engine that implements the service verifies that the collected data conform to the regulatory requirements as expressed through the respective policies. It generates reports about the verification of compliance available through the CAS (Compliance Auditing Service) GUI.

- Risk Assessment Service: it checks the target IoT deployment against a set of known vulnerabilities databases, like NIST’s NVD or CVSS. The service operates on the collected security data for the target IoT deployment as well as stored CTI data. The Risk Assessment Engine tries to match patterns of vulnerabilities against the collected data and in case it discovers that the IoT deployment is exposed to a vulnerability, it raises an alert.

This architecture provides the background environment/context where the SLA management and monitoring services will be implemented. Indeed, one of the next sections in this deliverable introduces extension and enhancements to the SecureIoT architecture in order to accommodate the SLA monitoring and management requirements.

1.4 Methodology

This deliverable is the first step towards the implementation of SLA management mechanisms as part of the SecureIoT platform. It will specify the functionalities of SLA management in SecureIoT, while at the same time aligning to main business scenarios and the SecureIoT architecture. A subsequent version of the deliverable (i.e. deliverable D3.10) will report on the practical implementation of the SLA management mechanisms in-line with specifications of the present
deliverable. The implementation will take advantage of modules and functionalities of the SecureIoT architecture. An overview of the part and methodology followed for the specification and implementation of SLA management mechanisms in SecureIoT is provided in the following figure.

Figure 2: Methodology and Main Activities Entailed in the Specification and Implementation of SLA Management in SecureIoT

As evident from the figure, the implementation of the SLA management mechanisms in the coming deliverable (D3.10) will be greatly facilitated by the specification of appropriate data entities in the SecureIoT security data model, which will be destined to support the management of SLAs.

1.5 Relationship to other Deliverables

The present deliverable is closely related to the deliverable of the SecureIoT architecture, as well as to other deliverable of WP3 which deal with security data collection. It can also serve as input to the exploitation deliverables in WP8 of the project, since it highlights the business interactions between IoT system owners/operators that wish to protect their systems and the providers/operators of SecureIoT security solutions in the form of SECaaS services. In particular, the present deliverable is directly linked to the following documents/reports of the project:

- D2.5, “Architecture and Technical Specifications of SecurityIoT Services_Final version”, given that the implementation of the SLA management solution will be aligned to the SecureIoT architecture.
- D3.2, “Security Information Storage and Analytics Infrastructure_Final version”, since the SLA information will be persisted/stored in the Big Data infrastructure of the project, which is also developed in WP3.
- D3.5, “Intelligent Data Collection Mechanisms and APIs_Final version”, as the SLA management mechanisms can benefit from the intelligence of the data collection mechanisms.
• D8.7, “Exploitation and Business Planning Activities_Interim version”, given that the business actors and interactions specified in this deliverable in relation to the SecureIoT services could serve as a basis for defining the details of possible business models for the exploitation of the SecureIoT platform and its SECaaS services.

1.6 Document Structure
The deliverable document is structured as follows:

• Section 2 gives the motivation for the support of SLA management, including relevant business scenarios and interactions between stakeholders that are subject to SLAs.
• Section 3 provides the main specifications of the SLA management module of the SecureIoT project, while highlighting the main parameters of SLAs that will be tracked and managed.
• Section 4 illustrates how the SLA management functionalities are implemented in the scope of the SecureIoT architecture. It introduces new building blocks in the SecureIoT architecture, along with enhancements to the SecureIoT security models, notably enhancements that are destined to support SLA management.
• Section 5 concludes the document.

Note that the deliverable includes an Appendix which details the structure of SLA-related enhancements within the SecureIoT Data Models.
2 Motivation for SLA Management

2.1 The SecureIoT SECaaS Services

The SecureIoT SECaaS services have been discussed in section 1.2 and include:

- **Risk Assessment:** a set of services for the quantification of risks to which an IoT deployment or application may be exposed to, based on the probability and impact each one may have. The NIST CVSS (Common vulnerability Scoring System) will be used for this service.

- **Compliance Auditing:** a set of services that support auditing of IoT deployments and services against existing sets of security and privacy controls. Auditing services depend on data collected from the IoT deployment as well as output of analytics from their processing. Auditing requirements may include policies that need to be complied with and may also be expressed in XACML. The auditing service outputs sets of recommendations about issues in which compliance may be at risk and require further attention.

- **Developer Support:** a set of services for secure IoT programming based on programming annotations that extend and complement existing programming constructs. The services are expressive enough to allow for enforcement of policies at various levels of the IoT target deployment, i.e., device, smart object, edge, cloud. The developer support services are automatically mapped into controls of the target IoT deployment or application and are used during its operation.

Table 1 summarizes the security services that are provided by the SecureIoT platform.

Note also that as part of WP5 of the project, SecureIoT is also developing a knowledge base of IoT security information such as threats, vulnerabilities, attacks and more. This knowledge base could be also assessed as a service and hence could be considered as one of SecureIoT services that are subject to be regulated by an SLA.

The above-listed services are meant to be add-ons to the IoT application deployment to which they are applied, as opposed to built-ins into it. The advantage of providing external security services is that they can be designed, developed and enhanced independently of the application to which they are used. In essence these services are an abstraction and they evolve from the security requirements that accompany a number of representative IoT applications and are packaged as external services, like the SECaaS of SecureIoT. Moreover, extensions, adaptations and enhancements to the security services can evolve in a unified way so that these services are applicable to a wide range of IoT applications.

In principle, each add-on SECaaS service receives some (input) data from an IoT system and returns (as output) security information and/or actionable intelligence. The following table illustrates at high level the inputs and outputs of the SECaaS services, which will drive the specification of the information that will be managed by the SECaaS SLAs.
### Table 1: Input and Outputs of the SECaaS Services

<table>
<thead>
<tr>
<th>SecureIoT SECaaS Service</th>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>Data about asset attacks of the IoT system provided by the Analytics subsystem.</td>
<td>Risk Assessment Report for specified assets of the IoT system, including grading of the risks</td>
</tr>
<tr>
<td>Compliance Auditing</td>
<td>Data about assets of the IoT system provided by a number of probes</td>
<td>Compliance Auditing Report, including points of compliance and non-compliance</td>
</tr>
<tr>
<td>Developers Support</td>
<td>Data about assets and security policies provided as static data and through a number of probes</td>
<td>Enforcement of policies at the level of different assets (e.g., devices, services, platforms) – Report on the outcome of the enforcement</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>Data about the IoT system provided through probes</td>
<td>Resolution of possible threats, vulnerabilities and attacks</td>
</tr>
</tbody>
</table>

An SLA between the different business entities that are involved in a SECaaS service will therefore monitor information associated with the above listed inputs. Furthermore, it is expected that SecureIoT will be able to audit and enforce constraints regarding the quality and the quantity (e.g., data volumes) entailed in the SLA as far as the above-listed inputs and outputs are concerned.

The present document focuses among others on one such extension of the basic SecureIoT security services, in particular, their provision over an environment in which several IoT platform owners/operators need to collaborate for supporting an IoT application.

The key advantage of supporting security services for applications that may be deployed over multiple IoT platforms is that a more integrated view of vulnerabilities and related risks can be modelled.

### 2.2 Business Actors entailed in SecureIoT Services

The offering of SecureIoT services involves at least two actors:

- An entity operating an IoT system and providing security data about it.
- Another entity processing these data and providing a security service based on the SECaaS modality.
It is also possible that more stakeholders are engaging in the business case of SECaaS services provision, as for example in scenarios involving multiple IoT platforms.

The following table illustrates various business actors that could be involved in SECaaS services provisioning, along with their relevance to the SecureIoT SLA management functionalities.

Table 2: Overview of Business Roles Entailed in the Provision of an IoT SECaaS Service and Associated SLA Management Functionalities

<table>
<thead>
<tr>
<th>Business Actor</th>
<th>Description</th>
<th>Example of SLA Rationale and Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT System Operator</td>
<td>An individual or enterprise in charge of the operation of an IoT system comprising one or more IoT platforms and devices</td>
<td>The operator needs to secure the operation of its systems based on a set of proper SECaaS services. It therefore engages in an SLA with the SecureIoT services provider.</td>
</tr>
<tr>
<td>IoT Platform Provider</td>
<td>Vendor of an IoT platform that enables the provision of IoT services based on a number of IoT devices that are integrated to the platform.</td>
<td>The platform provider needs to augment its platform based on IoT security features and functionalities. It therefore integrates the platform with SecureIoT services based on an SLA with the SecureIoT services provider.</td>
</tr>
<tr>
<td>IoT Device Vendor</td>
<td>Vendor of a device e.g. OEM (Original Equipment Manufacturer)</td>
<td>The OEM needs to secure its device without deploying computationally expensive security functions on it. To this end, it accesses SecureIoT services based on a SECaaS delivery modality and subject to a proper SLA.</td>
</tr>
<tr>
<td>IoT Services Provider</td>
<td>A business entity that provides IoT services over a single or multiple IoT platforms (e.g., IoT cloud platforms). It is likely to be an SME integrating and offering services over a provider’s infrastructure.</td>
<td>The services provider needs to offer added-value protection for its services based on advanced functionalities like data-driven security intelligence and advanced risk assessment. It can access them as a service (i.e. SECaaS) based on an SLA with a SecureIoT services provider.</td>
</tr>
<tr>
<td>IoT Developer</td>
<td>An individual or enterprise that develops IoT applications using third-party infrastructures (e.g. a PaaS infrastructure offered by an IoT platform provider)</td>
<td>The developer benefits from a secure IoT programming service such as the developers’ support service offered by SecureIoT based on a SECaaS modality. This is subject to an SLA with the SecureIoT services provider.</td>
</tr>
</tbody>
</table>
SECaaS Service Provider | Business entity in charge of providing and operating a specific SECaaS service that is accessible to organizations wishing to secure their IoT devices or services. | The SECaaS service provider establishes an SLA with IoT service providers, IoT developers and other business entities that wish to access its SECaaS service. The SLA regulates the operation of the service, including the rights and obligations of the parties.

SecureIoT Platform Operator | A entity operating the entire SecureIoT platform, which offers various data-driven SECaaS services. | The SecureIoT platform operator establishes SLAs with business entities (e.g., IoT Services Providers, OEMs) that use its SECaaS services. Each SLA regulates one or more services provided to some of the above listed business entities.

2.3 Indicative Business Scenarios involved SLAs and their Management

In following paragraphs, we illustrate some business scenarios involving SECaaS services and the role of SLA management for their realization. The aim of these scenarios is to illustrate the above-listed business roles, along with the way they take advantage of the SecureIoT SECaaS services.

2.3.1 Scenario #1: SECaaS Services for IoT Device Protection

An OEM has built and is providing an IoT device such as a sensors’ gateway. The OEM intends to offer increased security for its device through bundling a SECaaS with it. It offers this SECaaS service (e.g., a dashboard visualizing risk assessments and alerts) based on partnership with a SECaaS provider. This partnership is subject to an SLA specifying and regulating the relationship between the OEM and the SECaaS provider. The latter can use the SecureIoT platform to offer this SECaaS service.

As illustrated in Table 2, the SECaaS service could be offered/provided to the owner/user of the device i.e. an entity that has purchased this device from the OEM. In both cases, the SLA regulates parameters like the volume and frequency of data provision from the OEM vendor to the SECaaS provider, as well as parameters associated with the SECaaS service itself like the number and type of risk assessments of the device and the frequency they will be provided to the other party (i.e. OEM or device user/owner).
2.3.2 Scenario #2: SECaaS Services for IoT Platform Protection

An IoT platform provider hosts and provides a range of IoT services to different customers. The services are provided in the cloud, based on a PaaS or SaaS (Software as a Service) modality. The platform provider establishes an SLA with a SECaaS provider (i.e. an entity using SecureIoT platform) in order to protect the devices and services that are integrated with its cloud-based platform. Hence, the platform provider can offer and visualize risk assessments, security alerts and security compliance reports to its customers. Likewise, it can take advantage of SECaaS reports as part of its efforts to secure its infrastructure and hosted services.

Figure 4 depicts at high level the interaction between the IoT platform provider and the SECaaS provider, along with the role of the SLA. It also explains how the SECaaS service can be provided to the end-user of IoT applications i.e. the customers of the IoT platform provider.
2.3.3 Scenario #3: SECaaS Services for IoT Development
An IoT developer programs IoT devices including smart objects like robots and drones. Likewise, the IoT developer develops IoT services using multiple of these devices and integrating them in a private or a public cloud infrastructure. In order to secure the IoT services that he/she is developing, the developer uses annotations that are supported by the SecureIoT platform, which enable the developer to apply/enforce security policies in a distributed manner. To this end, the developer has an SLA with the SecureIoT service provider.

2.3.4 Scenario #3: SECaaS Services for IoT Service Protection
This scenario can be considered a special case of the IoT platform protection scenario, as one or more IoT services can be offered through an IoT platform that can be secured through the SecureIoT SECaaS service. However, it is also possible to apply a SECaaS to an IoT service provider that does not rely on a public cloud for its service offering, but rather on an alternative set of devices, edge gateways and data centre infrastructures. Another alternative scenario involves the protection of IoT services that span multiple IoT platforms, which can be the case for composite supply chain services (e.g., a product traceability service) that involve multiple stakeholders. This alternative case is elaborated in the following paragraph.

2.3.5 Scenario #4: SECaaS Multi-Platform Protection
IoT applications may in general be deployed on multiple IoT platforms. Examples include applications that monitor the supply chain, applications for smart cities, traffic monitoring and control and so on. This section presents an example of a multi IoT platform application for monitoring the supply chain of goods and focuses on the interactions between the IoT platform owners/providers and the SecureIoT platform that provides the security services to the application.
The scenario is depicted in Figure 5. It involves multiple stakeholders that are involved in the production and final distribution of goods. Each one of those will typically use its own IoT platform for collecting data related to the amounts of raw material, goods production phases and states, forwarding of goods and warehouse state for their final distribution. The respective IoT platforms will collect status data from deployed sensors and will forward them to the IoT application. The IoT application will typically make use of the collected data to provide a unified view of the chain and the status of the goods to its users.

For the SecureIoT platform to provide its security services to the IoT application, it needs to collect security data from the involved IoT platforms and the application itself. Therefore, probes must be deployed to the monitoring devices, the involved IoT platforms and the IoT application for security data collection. The collection and transfer of sensitive security related data is a task that may face the scepticism of IoT platform owners/operators as sensitive data are to be exposed to a third party (SecureIoT service provider). Therefore, the interactions between the IoT platform owners/operators and the SecureIoT service provider have to be covered under precise Service Level Agreements. The SLAs that govern the interactions between the IoT platform owners/operators and the SecureIoT service provider will certainly be specialized to the application at hand but also refined to the appropriate level of detail. A typical SLA will specify the obligations of the parties involved as follows:
1. The IoT platform owner/operator has to provide an amount of security related data to the SecureIoT service provider per unit of time. That amount may range between a minimum and a maximum threshold.

2. The SecureIoT service provider has to provide security alerts to the IoT platform owner/operator when detected.

3. A service fee has to be applied for each period of SECaaS service usage.

4. Clauses may also be specified in the sense that if an attack to the IoT application goes undetected then damages should be recovered.

In such an SLA the amount of collected security data may be adjusted to the service level required. Obviously, the more security data provided to the SecureIoT service provider, the more precise the service and quality of alerts generated by it.

Multi-platform services scenarios entail more complex business and technical relationships between SecureIoT services providers and other stakeholders, as multiple SLAs need to be established, managed, and correlated. However, despite the existence of multiple IoT service providers, these SLAs could be virtualized and appear as consolidated.
3 Functional Specifications of SLA Management in SecureIoT

3.1 Overview

The SecureIoT SLA management module aims at facilitating the establishment and tracking of SLAs in the scope of SECaaS services provided by the SecureIoT platform. It is in charge of the following functionalities:

- **Definition and Activation/Establishment of an SLA.** In the scope of the actual operation of the SecureIoT platform, an SLA shall be established between the stakeholders involved in the provision of the SECaaS services and their IoT systems. The definition and establishment of the SLA will effectively setup a contract that will regulate the rights and obligations of two or more business entities as part of the provision of the SECaaS services.

- **Monitoring and tracking of the SLA.** The SLA management module will monitor the execution and operation of the SLA. This requires auditing that the mandates of the agreement are met by the participating parties. The monitoring and tracking of the SLA encompasses elements of usage control, as the SLA management module will ensure that data and reports exchanged between the parties are as agreed.

- **Deactivating the SLA.** The lifecycle of the SLA ends when the parties decide to deactivate it, in which case it goes out of scope.

The following paragraphs illustrate the main functionalities of the SecureIoT SLA management module. They also describe its design and implementation in-line with the SecureIoT+ architecture. Note however, the SLA management module is meant to provide a proof of concept of the SLA management functionalities rather than an exhaustive commercial scale implementation. Parameters and functionalities specified in the following paragraphs are designed in this context.

3.2 SLA Management Module Specification

3.2.1 Identification – SLA ID

Each SLA shall be uniquely identified within the SecureIoT platform i.e. upon its creation it should be associated with an identifier. Furthermore, it is associated with a time window of validity, which starts counting from the time the SLA is activated (see following paragraphs).

3.2.2 Participating Entities

The SLA management module shall keep track of the business entities (i.e. typically organizations) that commit to the SLA. In every given SLA at least two entities shall participate:

- **SECaaS Customer:** The entity providing security-related data and receiving a SECaaS service.
• **SECaaS Provider**: Another providing the results of a SECaaS service (e.g., compliance reports) following the reception of security related data from IoT systems of the other party.

In the case of multi-platform IoT services, the SLA might engage more than one SECaaS Customer or alternatively the single SECaaS customer could correspond to a set of collaborating organizations.

### 3.2.3 SLA Type

In line with the SLA lifecycle outlined above, each SLA within the SecureIoT platform shall be associated with one of the following statuses:

- **DEFINED**: This status denotes that the SLA has been defined but is not activated yet. The SecureIoT platform keeps it in the list of SLAs but does not take any action/activity about it. At this stage, the participating parties could make changes in the SLA.
- **ACTIVE**: This status denotes that the SLA is active within the SecureIoT platform. This means that the SecureIoT platform will monitor the SLA, report about it and enforce any measures stemming from it.
- **INACTIVE**: This status denotes that the SLA is currently deactivated, yet it was previously active. An Inactive SLA cannot be updated (e.g., in terms of its parameters), but it can be reactivated i.e. revert to the ACTIVE state.
- **DELETED**: This status denotes that the SLA has gone out of scope of the SecureIoT system e.g., because the parties decided to create a new one. It is still maintained in the system for statistical, administrative and logistics purposes, yet it cannot become active again.

In support of the above-listed status and lifecycle, the SLA management module shall support CRUD (Create Read Update Delete) operations for objects and/or data structures representing SLAs within the SecureIoT platform.

### 3.2.4 SECaaS Services Type

Each SLA shall keep track of the SECaaS services types associated with it. In-line with the SECaaS services that are provided by the SecureIoT platform, the following types shall be supported:

- **Risk Assessment SECaaS**.
- **Compliance Auditing SECaaS**.
- **Developers Support SECaaS**.

The SLA Management module could however be extensible in terms of SECaaS service types in order to support additional types of SECaaS services in the future.

### 3.2.5 Tracking of Data Collection Information

The SLA management module shall track information about the data provided by the SECaaS Customer(s) to the SECaaS provider, including:
3.2.6 Tracking of SECaaS Outputs

For each SLA, information about the SECaaS output shall be maintained and tracked. This information shall include:

- **Total Reports.** The total number of reports provided by the SECaaS provider to the SECaaS customer for the duration of the SLA.
- **Minimum Frequency of Reports.** The minimum frequency at which the SECaaS provider is expected to provide a report to the SECaaS customer.
- **Push/Pull Mode.** This parameter denotes whether the reports should be provided in a push or pull mode (or both).

3.2.7 Notifications & Alerts

The SLA management module should be notified in case of new reports issued by the SECaaS services. Hence, a push and pull mode for acquiring statistics and usage information associated with the SECaaS services should be supported.

3.2.8 Reconfiguration

SLAs should be reconfigurable, in the same way the SecureIoT probes are reconfigurable. Hence, the security analytics of the SecureIoT platform may indicate the reconfiguration of one or more SLAs in order to provide intelligence in the business interactions of SECaaS Customers and SECaaS Services providers.
3.2.9 Accounting and Utility Metrics

The SLA management module shall maintain and keep track of a range of utility metrics including:

- The duration of the SLA i.e. the time the SLA is valid.
- The number of reports provided by the SECaaS services in different time windows (e.g., per day, per week, per month).
- The data volume processed by the SECaaS provider in order to provide the SECaaS service, measured in bytes.
- The number and type of probes providing data to the SECaaS provider.

These parameters can serve as a basis for accounting and pricing of the SLA. Nevertheless, other pricing options will be supported such as flat (monthly or weekly) pricing. In principle these are parameters already used in cloud computing and IoT services [Calbimonte14].

As explained in following paragraphs, utility metrics can be used to implement incentives for SECaaS customers to provide more security-related data, that SECaaS providers could use to improve the accuracy and functionality of their services.

3.2.10 Security Requirements

The implementation of the SLA Management module should be itself secure, by fulfilling the following requirements:

- Collected security data should be guaranteed for their authenticity. For this purpose, techniques like digital signatures may be employed.
- Collected security data have to be communicated confidentially from the probes to the SecureIoT platform. Encryption and decryption techniques should be used for this purpose.
- The integrity of the collected data that are transmitted to the SecureIoT platform has to be secured. For this reason, hashing techniques shall be used for guaranteeing the integrity of the transferred data.

3.2.11 Other SLA Information

A wide range of additional parameters can be tracked as part of an SLA implementation. Some of these parameters include:

- Number of users of SECaaS services and their SLAs, including details about their type (e.g., defined/registered, active, deactivated etc.).
- Number of users and SLAs currently logged in and/or active.
- Statistics about up time and down time in a given time window (e.g., last day, week, month, quarter, year). This can be used to prove that commitments associated with the cloud service and infrastructure that supports the SECaaS are respected.
- Number of SECaaS transactions processed in a given time window (e.g., hour, day, and week).
Utilization rates and statistics for a given time window (e.g., latest minutes, hour, and day).

Reports on SLA reports produced, including full information about each report such as the name of the report, the date & time that it has been running, the business entities involved and more.

Some of the above metrics are optional, while most of them fall in the realm of cloud service provision and are not directly related to IoT security. As already outlined, in the design of the SLA processing engine, we have primarily focused on parameters and reports that pertain to SecureIoT and SECaaS services, rather than on conventional cloud computing parameters handled by the cloud provider.

### 3.2.12 Business Incentives Tracking & Implementation

The utility metrics outlined above could also provide a way for implementing incentives schemes for IoT system operators (including SECaaS customers) to provide data to SECaaS providers. In principle, a SECaaS customer provides security related data to a SECaaS provider as a prerequisite for the delivery of the SECaaS service. However, SECaaS customers may opt to provide more or less data as part of an SLA, as part of the following trade-off:

- SECaaS customer would like to limit the amount of data that they provide as they usually perceive their data as an asset that should be kept private/confidential.
- SECaaS providers would like to access as much data as possible, in order to appropriate train algorithms and provide more accurate and credible SECaaS services.

Incentives schemes can be used to balance and resolve this trade-off. They may involve:

- Discounted prices for SECaaS customers that provide more data than the minimum needed for the provision of the service.
- Added-value security services for SECaaS customers that provide more data than the minimum needed. Such added value services can be based on the collection of credits for SECaaS customers that provide more data that agreed.

In the scope of the SLA management functionalities of the project, such schemes can be implemented based on the following simple rules:

- **Discounts**: Provide X% discount for the provision of Y% additional data, over the minimum specified in the SLA.
- **Added-Value Security Services**: Give Y credits to a SECaaS customer for every X% additional data over the minimum specified in the SLA. Accordingly, exchange an amount of credits with added-value functionalities (e.g., the provision of more and/or richer reports).
4 SLA Management Design and Implementation

4.1 SLA Management Module Data Models

In order to support the above-listed SLA management functionalities, SLA information is included as part of the SecureIoT data model. In particular, the SecureIoT data model has been enhanced with a new group of objects that is dedicated to SLA management. It includes all parameters outlined above (e.g., SLA status, creation/activation timestamps, data volumes, total number of SECaaS reports, types of SECaaS reports), along with proper links to existing objects and types of the SecureIoT data model. The SLA-enhanced SecureIoT data model will serve as a basis for SLA representation and management. Note that in other contexts (e.g., cloud-based applications) domain specific languages and representations have been introduced for representing and managing SLAs (see for example [Uriarte14] and [Kearney10]).

In SecureIoT we opted for an XML-based representation of SLA information in-line the SecureIoT security model. As outlined in earlier SecureIoT deliverables of this workpackage, the SecureIoT data model serves as a basis for reflecting the status of the IoT system, including information about security data and services that relate to its assets. Hence, it enables monitoring of the status of the security platform, as well as its configuration. In this context, the enhancement of the SecureIoT data model with information about SLAs provides the means for configuring and visualizing SLAs. In this SLA-enhanced version of the SecureIoT platform, SLAs are an integral part of the platform and its configuration and management capabilities.

The detailed structure of the enhanced version of the SecureIoT Data Model is presented in Appendix A. As shown in Appendix A, the objects represented in the SLAs, are nested within the root of the SecureIoT data models in a dedicated group. Dedicated objects are also foreseen for SLA reports.

4.2 Integration in the SecureIoT Architecture

A new SLA Processing Engine module is introduced in the SecureIoT architecture. It is primarily in charge of maintaining information about the SLAs that are active in the platform up to date. This information is persisted and managed in a dedicated part of the Global repository of information of the SecureIoT platform. It is can also monitor and audit whether the SLA is enforced from the participating actors and their systems. To this end, the SLA Processing Engine needs to access information from various modules of the SecureIoT platform. This is performed using the very same probes mechanisms that SecureIoT exploits in order to access/collect security data from the IoT systems that it protects. However, there is one major difference: The SLA Processing Engine takes advantage of “internal” SecureIoT probes i.e. probes that are deployed within the platform in order to collect information from other modules of the platform, such as other probes, the security analytics and the modules implementing the various SECaaS services. These probes are indeed different from the “external” probes used to collect...
information from external systems, as they are part of the SecureIoT platform, rather than residing outside of it.

The exploitation of the probes mechanism provides a uniform way for managing the data/information collection of the SLA Processing Engine. In particular, probes can be flexibly configured, deployed and (un)deployed, as new services are added in the SecureIoT platform, given that the addition of a new SECaaS service instance is always accompanied with a new SLA instance. Furthermore, the established probes mechanisms provide readily available interfaces specifications for the purpose of SLA-related data collection.

Figure 6: SecureIoT Architecture Enhanced with the Building Blocks for SLA Management

Figure 6 illustrates the SecureIoT architecture with enhancements for SLA management. The main enhancements include:

- **SLA probes** in different parts/layers of the SecureIoT architecture, including probes in the Data Management, Analytics and Risk Assessment Groups. These probes enable the acquisition of (raw) data that are sent to the data routing component.

- **Enhancements to the Data Routing component**, in order to transform raw data to properly structured Observations and to store them to the Global Repository (Observations Repo).

- **An SLA Processing Engine** that processes raw data and generates SLA reports. The latter are stored in a dedicated part of the Global Repository destined to support SLA Management, which is conveniently called (SLA Repo).
• The SLA Repo that hosts SLA reports along with configuration data about each SLA.

• The SLA Admin Console, which provides the means for configuring and managing SLAs, based on the processing of configuration data of the SLA Repo.
5 Conclusions

This deliverable has presented the project’s initial approach to the management of Service Level Agreements for the SECaaS services of the project. SLA management functionalities are not prerequisite for the technical validation of the SECaaS services, but they are necessary for their operation in pragmatic business contexts. In SecureIoT SLAs will be established between two of parties that can represent different business actors (e.g., IoT platform providers, OEMs, IoT service providers) depending on whether the SECaaS service is offered at the device, platform or service levels. The SLA reflects the rights and obligations of the business entities that participate in the delivery of a SECaaS service. In principle, the SECaaS Customer commits to providing security data to the SECaaS provider, while the SECaaS provider commits to provide security services (e.g., risk assessment reports) at a certain density/frequency.

As part of this deliverable, we have specified the main parameters that should be associated with the creation and management of an SLA. These include a range of utility metrics (e.g., data volumes, number of reports, and duration of the service provisioning) that can be used as a basis for accounting and charging in the scope of the SECaaS pay-as-you-paradigm. These parameters have been properly modelled in an SLA management data model, which has been integrated within the SecureIoT data modeling approach.

In practice, SLA management in SecureIoT will be implemented as part of the SecureIoT architecture and platform implementation. To this end, a new module for SLA Management has been specified as part of the SecureIoT architecture, which interfaces to all the logical layers of the SecureIoT platform. This module leverages the probes mechanisms as a means of collecting the information required for managing SLA.

The next version of this deliverable is expected to specify enhanced SLA management functionalities including more configuration and auditing functionalities for a wider spectrum of business scenarios involving SECaaS services. Even though the SLA management deliverables of the project are prescribed as reports in the SecureIoT DoA, the consortium will provide a small-scale proof of concept implementation subject to the specifications provided in this document. This implementation will be fine-tuned and enhanced as part of the second version of the deliverable. Moreover, in the final version of the deliverable we will provide concrete examples on the use of incentive-based schemes, including schemes resulting in reduced pricing of the services and schemes that provide value added SECaaS services to SECaaS customers that opt to provide more data than the minimum required for the delivery of a SECaaS service specified in their SLA.
References


Appendix A. SLA Data Models Structure

Figure 7: Structure of SecureIoT Data Model (SecIoT-DM) and placement of SLA group in it
Figure 8: Structure SLA Group – SLA Root Element
Figure 9: SLA Object Definition
Figure 10: SLA Object
Figure 11: Complex SLA Object
Figure 12: Structure of SLA Report